Abstract

An extremely secure method for keying source contents to a source storage medium provided to prevent use of unauthorized copies at minimal cost. The host processor combines a unique, immutable and verifiable physical attribute of a hard disk drive, i.e., the drive's defect list, with the content to be secured to write a corresponding fingerprinted encrypted content on a source medium. When a local processor wants to use the sanctioned source content, the fingerprinted content is read from a local storage medium. The local processor then decrypts and separates the defect list out of the source content and reads the local storage medium defect list. If the decrypted defect list matches the local storage medium defect list, then the local processor recognizes the local sanctioned medium and continues processing that source contents. Otherwise, a non-matching defect list comprises an unauthorized copy from the source to the local storage medium.